

**CISA Tabletop Exercise Package Dams Sector – Hydropower Facilities**

[Enter Organization Name]

<Exercise Date>

Updated March 2024

Cybersecurity and Infrastructure Security Agency

Table of Contents

[Handling Instructions 3](#_Toc158021094)

[Exercise Overview 5](#_Toc158021100)

[General Information 6](#_Toc158021101)

[Module 1 8](#_Toc158021102)

[Module 2 10](#_Toc158021103)

[Appendix A: Additional Discussion Questions 12](#_Toc158021104)

[Appendix B: Acronyms 15](#_Toc158021105)

[Appendix C: Case Studies 16](#_Toc158021106)

[Appendix D: Malicious Activity 17](#_Toc158021107)

[Appendix E: IT and OT Risk Mitigation 18](#_Toc158021108)

[Appendix F: Contacts and Resources 20](#_Toc158021109)

# Handling Instructions

**Delete instructions that are not applicable.**

TLP:CLEAR

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as “*Traffic Light Protocol (TLP):CLEAR*”: Recipients can spread this to the world; there is no limit on disclosure. This designation is used when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. **Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.**

This document may be disseminated publicly pursuant to TLP:CLEAR and <exercise sponsor name or other authority> guidelines.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP:GREEN

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as “*Traffic Light Protocol (TLP):GREEN*”: Limited disclosure, recipients can spread this within their community. This designation is used when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. **Note: When “community” is not defined, assume the cybersecurity/cyber defense community.**

This document should be disseminated to applicable partners and stakeholders on a need-to-know basis pursuant to TLP:GREEN and <exercise sponsor name or other authority> guidelines due to the sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP:AMBER

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as “*Traffic Light Protocol (TLP):AMBER”:* Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. This designation is used when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

This document should be disseminated to applicable partners and stakeholders on a need-to-know basis pursuant to TLP:AMBER and <exercise sponsor name or other authority> guidelines due to the sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP:AMBER+STRICT

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as *“Traffic Light Protocol (TLP):AMBER+STRICT*: Limited disclosure, recipients can only spread this on a need-to-know basis within their organization. Note that “*TLP:AMBER+STRICT”* restricts sharing to the organization only. This designation is used when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organization involved. Recipients may share TLP:AMBER+STRICT information with members of their own organization, but only on a need-to-know basis to protect their organization and prevent further harm.

This document should be disseminated to applicable partners and stakeholders on a need-to-know basis pursuant to TLP:AMBER+STRICT and <exercise sponsor name or other authority> guidelines due to the sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP:RED

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as “*Traffic Light Protocol (TLP):RED*”: For the eyes and ears of individual recipients only, no further disclosure. This designation is used when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.

This document should be disseminated to applicable partners and stakeholders on a strict need-to-know basis pursuant to TLP:RED and <exercise sponsor name or other authority> guidelines due to the extreme sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

# 

# Exercise Overview

|  |  |  |
| --- | --- | --- |
| Exercise Name | Exercise Name | |
| Exercise Date, Time, and Location | Exercise Date  Time (e.g., 9:00 a.m. – 12:00 p.m.)  Exercise Location | |
| Exercise Activities | Time | Activity |
| 20 Minutes | Threat Briefing and Opening Remarks |
| 60 Minutes | Module 1 |
| 20 Minutes | Break |
| 60 Minutes | Module 2 |
| 20 Minutes | Hotwash |
| Purpose | Examine the cyber resilience of <organization> in response to a significant cyber incident. | |
| National Institute of Standards and Technology Cybersecurity Framework Functions | Govern, Identify, Protect, Detect, Respond, Recover | |
| Objectives | 1. Examine the response capabilities of <organization> during a significant cyber incident. 2. Examine plans, policies, and procedures in response to a cyber incident. 3. Assess internal and external communications processes. | |
| Threat or Hazard | Cyber Incident | |
| Scenario | A network compromise resulting from an insider threat leads to the deletion of operation files, causing a shutdown of operations. | |
| Sponsor | Exercise Sponsor | |
| Participating Organizations | Overview of organizations participating in the exercise (e.g., federal, state, local, private sector, etc.). | |
| Points of Contact (POC) | |  |  | | --- | --- | | **Insert Organization POC(s)**  Contact Information | **CISA National Cyber Exercise Program (NCEP)**  [cisa.exercises@cisa.dhs.gov](mailto:cisa.exercises@cisa.dhs.gov)  **Dams Sector Risk Management Agency**  [damssector@cisa.dhs.gov](mailto:damssector@cisa.dhs.gov) | | |

# General Information

## Building Resilience

The purpose of the National Cyber Exercise Program’s CISA Tabletop Exercise Packages (CTEPs) is to increase your organization’s resilience by assessing and validating capabilities and identifying areas for improvement. The National Institute of Standards and Technology (NIST) defines cyber resilience as “the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.”[[1]](#footnote-2)

## Using this Situation Manual

Modules 1 and 2 contain the scenario injects and discussion questions you will use to conduct the exercise. The footnotes in the modules contain corresponding resources intended to guide your preparedness efforts. The appendices provide the following information to tailor the exercise discussion:

* Appendix A: Additional discussion questions that can replace or augment the existing Module 1 and 2 discussion questions.
* Appendix B: Reference section for acronyms used within this situation manual.
* Appendix C: Case studies that provide real-world examples of the threats presented in this scenario.
* Appendix D: An explanation of the malicious activity presented in this scenario.
* Appendix E: An overview of risk mitigation techniques for Internet Technology (IT) and Operational Technology (OT) systems.
* Appendix F: Additional cybersecurity preparedness and response resources.

## Participant Roles and Responsibilities

**Players** have an active role in discussing or performing their primary roles and responsibilities during the exercise. Players discuss or initiate actions in response to the scenario. Players may include IT/information security personnel, OT personnel, physical security and emergency management personnel, human resources and legal personnel, and any other personnel with a role in incident response.

**Observers** do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise. Observers may include senior-level leadership, IT/information security personnel, OT personnel, physical security/emergency management personnel, human resources and legal personnel, and any other personnel without a role in incident response.

**Facilitators** provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key Exercise Planning Team members may also assist with facilitation as subject matter experts during the exercise.

**Note-takers** are assigned to observe and document exercise activities. Their primary role is to document player discussions, including how and if those discussions conform to plans, policies, and procedures.

## Exercise Structure

This exercise is intended to be a multimedia, facilitated exercise. Players will participate in the following:

* Cyber threat briefing (if desired)
* Scenario modules:
  + **Module** **1:** This module introduces potential insider threat activity and issues with the Industrial Control System (ICS)/Supervisory Control and Data Acquisition (SCADA) Human Machine Interface (HMI) connection.
  + **Module 2:** This module continues the scenario with a decrease in power generation followed by deletion of control files, leading to an operational shutdown.
* Hotwash
* ***Structure Note:*** *Modules, timeline dates, and discussion questions included in each module may be modified as desired. Appendix A contains additional discussion questions for each module.*

## Exercise Guidelines

* This exercise is intended to be held in an open, no-fault environment. Varying viewpoints are expected.
* Respond to the scenario utilizing your knowledge of existing plans and capabilities, along with the valuable insights derived from your training and experience.
* Decisions are not precedent-setting and may not reflect your organization’s final position on a given issue. This exercise is an opportunity to discuss and present multiple options, possible solutions, and suggested actions to resolve or mitigate a problem.
* There is no hidden agenda, and there are no trick questions. The resources and written materials provided are the basis for discussion.
* In any exercise, assumptions and artificialities are necessary to complete play within the given time, achieve training objectives, and account for logistical limitations. Please do not allow these factors to negatively impact your participation in the exercise.

## Exercise Hotwash and Evaluation

The facilitator will lead a hotwash with participants at the end of the exercise to address any ideas or issues that emerge from the exercise discussions. The hotwash is held at the end of the exercise discussion. The hotwash is designed to provide an opportunity to discuss strengths and areas for improvement immediately following the conduct of an exercise.[[2]](#footnote-3)

# Module 1

### Day 1

The Cybersecurity and Infrastructure Security Agency (CISA), in partnership with the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI), issue a joint alert regarding threat actors using publicly available artificial intelligence tools to design malware targeting ICS/SCADA systems.[[3]](#footnote-4) Threat actors have used the malware to access sensitive files from the server and write files to the directory, resulting in code execution. Remote code execution has been used by malicious actors to control dam functions, including the opening and closing of sluice gates.

## Discussion Questions

Discussion questions included in each module are designed to explore different aspects of your operational resilience. The questions may be modified as desired. Additional questions can be found in Appendix A.

1. What are the greatest cyber threats to your operations?[[4]](#footnote-5)
   1. What are the possible impacts of an intrusion into your IT/OT systems?
2. What cybersecurity threat information does your organization receive?
   1. What are your primary sources of information?
   2. How do you determine what information is relevant to your equipment and operations?
   3. What threat information is most useful?
3. What actions would your organization take in response to a report like the one presented in the scenario?
4. Describe your organization’s asset management plan and how you prioritize critical assets.[[5]](#footnote-6)
   1. How does your organization maintain availability of key assets/functions?
   2. How often do you conduct/updated your asset inventory?

### Day 11

A [hydroelectric specialist/hydro technician/energy services technician] for your facility recently attended a conference and learned of an artificial intelligence (AI) large language model (LLM) designed for controlling and operating transformers, regulators, and motor-operated sluice gates. The engineer visits a well-known natural language processing (NLP) site and downloads the LLM, installing it onto their unencrypted work laptop and begins making remote corrections to the SCADA.

1. Describe your organization’s cybersecurity training program for employees.[[6]](#footnote-7)
   1. How often are employees required to complete this training?
   2. Describe the cross-training or the coordination between the IT and OT departments.
   3. What additional training is required for employees who have system administrator-level privileges?
   4. What type of training methods or approaches have you found most beneficial?
2. Describe your organization’s bring your own device (BYOD) policy.
3. Describe your organization’s network configuration and your approach to network segmentation of IT and OT systems.[[7]](#footnote-8)
   1. Describe your organization’s patch management and vulnerability management plans.
   2. Does your organization apply Zero Trust Architecture (ZTA)/zero-trust concepts?
   3. Describe your policies on remote access to the OT network.
   4. What security protocols (MFA, encryption, etc.) exist on your hardware?
4. What are your policies on requesting new software/hardware?[[8]](#footnote-9)
   1. What policies do you have to prevent an end user from downloading unauthorized items?

### Day 24

A couple of hours into the third shift, operators encounter an issue with establishing remote access to the control of the opening and closing of sluice gates. The ICS/SCADA repeatedly drops its connection, resulting in delays as operators must log onto the system each time to make changes.

1. How do employees report and log anomalous IT/OT activity?
2. How does your organization baseline network activity on IT and OT networks?
3. How do you distinguish between normal and abnormal traffic?
4. What are your next steps when abnormal activity is detected/reported?
5. What Indicator of Compromise (IOC) feeds does your organization use?
6. How do IT/OT and physical security teams coordinate their investigation/assessment into potential incidents impacting both physical and cyber security?
7. What tools (e.g., threat hunting, security audits) do you leverage as part of a proactive cybersecurity strategy?[[9]](#footnote-10)

# Module 2

### Day 30

Midway through the third shift, operators notice a marked decrease in power generation believed to be caused by a decreased flow of water through the turbines. Instrumentation confirms that water flow is decreased because the sluice gates are partially closed.

### Day 31

During operational shift turnover between third and first shifts, screens on several computers go blank as the computers reboot. As computers initialize, operators log on and notice multiple pre-programmed control files have disappeared from the network.[[10]](#footnote-11)

With several computers missing files, control over the gates is halted and gates are closed as a safety measure. The resulting halt in water flow stops production for the electric companies contracting with the dam for power.

## Discussion Questions

1. Discuss your organization’s procedures for declaring a cyber incident.
   1. What escalation criteria is defined in your cyber incident response plan?
   2. How is your Emergency Action Plan (EAP) integrated with your other incident response plans?
   3. How are activations of different plans coordinated during incident response?
2. What redundant systems exist for when primary systems are compromised?
3. Who can authorize use of alternate systems or procedures?
4. How long can you perform manual or alternate processes on your critical systems?
5. What resources do you have for additional staffing requirements?
6. Does your organization have backups of control files and other important files stored in a location separate from your primary working files/copies?[[11]](#footnote-12)
   1. How long would it take to restore primary files from backups?
   2. How frequently do you test restoration from backups?
   3. How long do you keep copies of archived files backed up?
7. Discuss your organization’s procedures for collecting and preserving data.
8. Who is responsible and what actions would they take based on the scenario?
9. What essential services are dependent on your facility (e.g., power production, drinking or irrigation water)?
10. How do these impacts to essential services / critical infrastructure impact your restoration priorities?
11. How sufficient are your organization’s current internal resources for responding to the cyber incidents in this scenario?
12. What additional resources outside of your organization are necessary for responding to the cyber incident?
13. What are the processes or procedures for requesting additional resources?
14. What external partners (e.g., CISA, FBI, vendors) would you contact for assistance?

### Day 33

An employee from your facility contacts the Federal Energy Regulatory Commission (FERC) and calls the enforcement hotline to report the issues at the dam. FERC contacts your facility and requests a report on what is occurring and associated impacts.

1. What information are you sharing internally (e.g., with employees, leadership)?[[12]](#footnote-13)
2. What information are you sharing externally (e.g., with customers, partners)?
3. What legal and regulatory notifications are required based on the scenario?
4. When are notifications made?
5. Who is responsible for making the notifications?

### Day 50

Following many days of restoring systems, your facility is back to full operational capability. Investigation confirms malware was embedded in the LLM that the [hydroelectric specialist/hydro technician/energy services technician] downloaded. Once in the system, the malware initiated a worm that replicated and spread throughout the system, targeting and deleting multiple types of files.

1. When does your organization determine a cyber incident is over?
2. Who makes this decision?
3. What changes will you implement to increase the resilience of your organization?[[13]](#footnote-14)

# Appendix A: Additional Discussion Questions

The following section includes supplemental organizational resilience discussion questions designed to guide exercise play. Questions are aligned with the NIST functional areas and organizational roles and responsibilities. Exercise planners are encouraged to select additional, applicable discussion questions for the chosen scenario to bolster participant conversation. *This instructional paragraph, as well as undesired discussion questions, should be deleted in the final version of the Situation Manual.*

## Cyber Resilience

1. Discuss how cyber preparedness is integrated with your current all-hazards preparedness efforts.
2. How often are your cybersecurity plans, policies, and procedures externally reviewed or audited?
   1. What were the most recent results and action items that followed?
3. Discuss your risk management strategy.
4. How is it developed/maintained?
5. What considerations are addressed in your risk management strategy (e.g., extended downtime, impaired functionality, loss of data, etc.)?
6. Does your organization maintain a risk register that is consistently reviewed and discussed at an executive level?
7. Describe your organization’s review process for your Cyber Incident Response Plan (CIRP).
8. How often is the CIRP reviewed?
9. Which individual(s) and department(s) are responsible for reviewing and updating the plan?
10. How are updates to the plan communicated to department or agency employees?
11. Discuss your supply chain concerns related to your IT/OT infrastructure.
12. What cybersecurity language is included within third-party vendor contracts?
13. How do you evaluate the cybersecurity posture of your vendors?
14. How often are contracts reviewed?
15. How do your service level agreements address cyber incident notification?
16. What is your method for tracking and identifying firmware vulnerabilities in your network?
17. How is the integrity of your critical data protected and validated?
18. What external entities have access to your data?
19. How would those entities report a compromise of their systems to your office?
20. What essential functions are impacted by the incidents described in the scenario?
21. If primary communications are compromised, how do you provide information to internal and external entities?
22. What policies and procedures does your organization use to decide when and how to restore backed-up data?
    1. How does your organization incorporate measures for ensuring the integrity of backup data before restoration?

## Accounts & Privileges

1. What are your organization’s policies or procedures for IT account management?
2. What are the protocols for establishing, activating, modifying, disabling, and removing accounts?
3. Describe your organization’s employee off-boarding process.
4. Is this process coordinated with IT and Human Resources (HR)?
5. What additional actions are taken if the employee’s termination is contentious?
6. How does your organization retrieve all information system-related property during the employment termination process (e.g., authentication key, system administrator’s handbook/manual, keys, identification cards)?

## Incident Identification

1. How are cyber incidents reported within your organization?
2. What would trigger the reporting requirements established by regulation, state law, and/or organization policy?
3. What training do employees receive regarding reporting requirements and your cyber incident response plan?
4. What cybersecurity incident escalation criteria is defined in your cyber incident response plan?
5. Who is responsible and what actions would they take based on the scenario?
6. Who needs to be notified internally and externally according to the plan?
7. When would leadership be notified?
8. Discuss your organization’s intrusion detection capabilities and analytics that alert you to a potential cyber incident.
9. What type of hardware and/or software does your organization use to detect and prevent malicious activity on your systems/network?
10. How often is your organization’s data reviewed?
11. How would you determine whether unauthorized manipulation of data occurred?

## Incident Response

1. What are your processes for collecting evidence and maintaining the chain of custody during a cyber incident?
2. At what point in the scenario would you contact law enforcement?
   1. How would a law enforcement investigation impact containment, eradication, and recovery efforts?
3. Are IT/OT system owners’ contact information documented in your response plans to ensure the correct personnel can be reached during a cyber event?
4. What are the processes for contacting critical personnel outside of core hours?
5. How do you proceed if critical personnel are unreachable or unavailable?
6. How would an incident at vendor(s) affect your organization if they have access to your information?
7. What are the notification requirements to your organization for incidents?

## Recovery

1. What post-incident activities would your organization conduct?
2. What actions would your organization take if your IT/incident response staff could not confirm the integrity of your systems/data?
3. What is the risk associated with reactivating critical business processes and systems?
4. Describe the process to completely rebuild these systems.
5. What factors do you consider when making these decisions?

## Training & Exercises

1. What training does your cybersecurity incident response team undergo to detect, analyze, and report malicious activity?
2. What additional training and/or exercise requirements do you require for your incident response staff?
3. How often does your organization exercise its CIRP?
4. Who is involved in the exercises?
5. What external agencies are involved in the exercise?
6. How do your organization’s training and exercise efforts address both physical and cyber risks?
7. How often do senior staff/leadership participate in a cybersecurity exercise?

## Senior Leaders

1. As a leader in your organization, what cybersecurity resilience goals have you set?
2. Describe your organization’s cybersecurity culture.
3. What cybersecurity training is required for senior leadership?
4. At what point would you activate your organization’s Security Operations Center/Emergency Operations Center?
5. What is your role during a cyber incident?
6. What information do you need to support your decision-making process?
7. What are the gaps in your cybersecurity workforce?
8. How does your organization recruit, develop, and retain cybersecurity staff?

## Public Information

1. Describe your organizational processes to respond to media reports and inquiries.
   1. How would you preserve and reinforce the public’s confidence and trust in your organization during a significant incident?
   2. Who is responsible/authorized to speak to the media?
2. What training do employees receive on reporting contact with the media?

## Legal

1. What is the role of the legal department during a cyber incident?
2. What issues need to be addressed based on the scenario?
3. What legal documents does your organization have for cyber incidents?

# Appendix B: Acronyms

|  |  |
| --- | --- |
| Acronym | Definition |
| AI | Artificial Intelligence |
| BYOD | Bring Your Own Device |
| CIRP | Cyber Incident Response Plan |
| CISA | Cybersecurity and Infrastructure Security Agency |
| CPG | Cybersecurity Performance Goals |
| CSF | Cybersecurity Function |
| CTEP | CISA Tabletop Exercise Package |
| EAP | Emergency Action Plan |
| FBI | Federal Bureau of Investigation |
| FERC | Federal Energy Regulatory Commission |
| HMI | Human Machine Interface |
| HR | Human Resources |
| ICS | Industrial Control System |
| IOC | Indicators of Compromise |
| IT | Information Technology |
| LLM | Large Language Model |
| NCEP | National Cyber Exercise Program |
| NIST | National Institute of Standards and Technology |
| NLP | Natural Language Processing |
| NSA | National Security Agency |
| OT | Operational Technology |
| SCADA | Supervisory Control and Data Acquisition |
| TLP | Traffic Light Protocol |
| USACE | United States Army Corps of Engineers |
| UAS | Unmanned Aircraft System |
| ZTA | Zero Trust Architecture |

# Appendix C: Case Studies

## Hydropower Producer Suffers Ransomware Attack

In March 2019, a major global aluminum producer and Norway’s third-largest hydropower producer was hit by an extensive cyberattack. The company powers its aluminum production operations with 20 hydropower plants, producing 10 TWh annually. A ransomware attack halted production at some of the company’s 170 plants, while the remainder of the plants were forced to revert to manual operations.[[14]](#footnote-15) A team of investigators determined that malicious actors weaponized an email attachment to install ransomware on an employee’s computer. The email was sent from a trusted customer. The ransomware attack compromised users within the company’s network, then captured administrative credentials, allowing the malicious actors control of the company’s IT infrastructure. The ransomware was deployed via a manual push from the company’s domain controllers. The company immediately decided not to pay the ransom and restored data from trusted backups. Rebuilding manufacturing-specific software took approximately three weeks, while other company user systems and cloud services took up to three months to restore.[[15]](#footnote-16) Norway’s national computer emergency response team and cybersecurity center indicated that the company in this incident was a victim of LockerGoga ransomware, family of encryption ransomware that frequently targeted industrial software during 2019–2021.[[16]](#footnote-17) The incident cost the company approximately $70 million in losses in 2019.[[17]](#footnote-18)

## Distributed Denial of Service Attack Against Hydropower Producer

In April 2023, a hacker group claimed responsibility for a Distributed Denial of Service (DDoS) attack against the world’s fourth-largest hydropower producer. According to news reports, the company suffered a DDoS attack that led to its websites and applications crashing. The company confirmed that no critical systems were attacked, and user data was not compromised.[[18]](#footnote-19) DDoS attacks overwhelm organization servers with a flood of “junk” traffic, or requests. The group NoName057(16) claimed they were responsible for the attack. The group is known to use the Bobik botnet for their DDoS attacks and seeks participation voluntarily through its DDoS tool.[[19]](#footnote-20) NoName057 also claimed responsibility for attacks against Canadian government websites and a number of other politically motivated DDoS attacks during the same time period.[[20]](#footnote-21)

# Appendix D: Malicious Activity

## Data Loss and Data Theft

Data theft and malicious data loss is a type of cybercrime where criminals gain access to sensitive and private information that is not meant to be shared publicly. This data can be as simple as names and addresses and escalate to operational script/code and proprietary research. Once the information has been ascertained the data is often copied and used to commit the crime of identity theft or as a way to exfiltrate money from victims. The economic and reputational impacts of data loss/theft on individuals and organizations can be significant. Losses can include damage to productivity, continuity of operations disruption, financial cost from investigation and recovery, financial costs due to lawsuits from customers, employees, or regulatory penalties, and overall reputational damage. To mitigate data theft/loss it is necessary to know what personal and sensitive information is on your network or systems, know who has access to it, encrypt sensitive information, implement firewalls, apply network segmentation, and ensure your CIRP and Communications Plan include response and notification procedures for data breach incidents.

### Additional Resources

* Protecting Sensitive and Personal Information (<https://www.cisa.gov/resources-tools/resources/protecting-sensitive-and-personal-information>)
* Cybersecurity and Physical Security Convergence Action Guide (<https://www.cisa.gov/resources-tools/resources/cybersecurity-and-physical-security-convergence-action-guide>)

## Insider Threat

An insider threat refers to the potential of an individual with authorized access or knowledge within an organization to cause harm. The threats posed by insiders include theft, espionage, violence, and sabotage involving technology, virtual reality, computers, devices, and the internet. Unintentional threats involve the non-malicious (accidental or inadvertent) exposure of an organization’s IT/OT infrastructure, systems, and data leading to unintended harm. On the other hand, intentional threats involve malicious actions conducted by insiders with malicious intent, using technical means to disrupt business operations, identify IT weaknesses, access protected information, or advance an attack plan through IT system access. Such actions may include altering data, inserting malware, or deploying other offensive software to disrupt networks and systems. To successfully mitigate insider threats and implement effective insider threat programs, it is necessary to detect and identify observable, concerning behaviors or activities, followed by the subsequent implementation of measures aimed at managing the risk of potential harmful actions.

### Additional Resources

* CISA Insider Threat Mitigation Guide (<https://www.cisa.gov/resources-tools/resources/insider-threat-mitigation-guide>)
* Insider Threat Mitigation (<https://www.cisa.gov/topics/physical-security/insider-threat-mitigation>)

# Appendix E: IT and OT Risk Mitigation

## Boundary Protection

One of the most fundamental characteristics of a secure ICS network is the design and deployment of boundary protection. Boundary protection is the electronic division between ICS and enterprise networks. If boundary protection is not developed thoroughly, access to ICS networks can be manipulated via enterprise networks and other internet connected devices. Inadequate boundary protection can also make it difficult to detect unauthorized activity on ICS systems. To mitigate threats against network boundaries, limit the number of external networks to the system; implement a managed interface for each external telecommunication service; deny network communications traffic by default and allow network communications traffic by exception; detect and deny outgoing communications traffic posing a threat to external systems; and enforce adherence to protocol formats. For more information on boundary protection refer to the resource below.

*Additional Resources*

* NIST SP 800-53, Rev. 5.1.1.: “System and Communications Protection (SC) – Boundary Protection”(<https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home?element=SC-07>)
* Layering Network Security Through Segmentation (<https://www.cisa.gov/sites/default/files/publications/layering-network-security-segmentation_infographic_508_0.pdf>)

## Principle of Least Functionality

The principle of least functionality states that information systems should be configured to provide only essential capabilities and restrict or prohibit the use of non-essential functions, such as ports, protocols, and/or services that are not a key part of the industrial control system.[[21]](#footnote-22) Systems which are not structured using this principle have increased vectors for malicious parties to access. To implement the principle of least functionality, configure information systems to provide only essential capabilities; limit component functionality to a single function per device; identify and remove unauthorized/unsecure functions, ports, protocols, services, and applications, and disable any that are authorized but not necessary.

*Additional Resources*

* NIST SP 800-171, Rev. 3.0.0: “03.04: Configuration Management” (<https://csrc.nist.gov/pubs/sp/800/171/r3/final>)
* NIST Guide for Security Focused Configuration Management of Information Systems (<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf>)

## Physical Access Control

Physical access to assets should be managed and protected. Unauthorized physical access to field equipment provides a malicious actor the opportunity to modify, delete, or copy critical device programs and firmware. Malicious actors can also gain access to ICS networks and steal or vandalize cyber assets. Additionally, unprotected physical access locations present threat actors with an opportunity to add rogue devices to capture and retransmit network traffic. To mitigate threats against physical access control locations, develop, document, and disseminate a physical and environmental protection policy; maintain a list of individuals with authorized access to the facility where ICS systems reside; enforce physical access authorization; control physical access; monitor physical access; maintain visitor access logs; and protect ICS system equipment from damage and destruction.

*Additional Resources*

* NIST Cybersecurity Framework, v2.0 (via NIST CSRC CPRT), PR.AA-06: Physical access to assets is managed, monitored, and enforced commensurate with risk. (<https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.AA-06>)
* Interagency Security Committee (ISC) Best practices for Facility Access Control (<https://www.cisa.gov/resources-tools/resources/isc-best-practices-facility-access-control>)
* Recommended Cybersecurity Practices for Industrial Control Systems (<https://www.cisa.gov/sites/default/files/publications/Cybersecurity_Best_Practices_for_Industrial_Control_Systems.pdf>)

Appendix F: Contacts and Resources

Federal Government Contacts

* CISA (contact: [central@cisa.gov](mailto:central@cisa.gov), <https://www.cisa.gov>)
* United States Secret Service (USSS) Field Offices and Electronic Crimes Task Forces (ECTFs) (contact <https://www.secretservice.gov/contact/field-offices>, <https://www.secretservice.gov/investigation/cyber>)
* Federal Bureau of Investigation (FBI)
* Field Offices (contact: <https://www.fbi.gov/contact-us/field-offices>)
* Internet Crime Complain Center (IC3) (contact: [http://www.ic3.gov](http://www.ic3.gov/))
* National Cyber Investigative Joint Task Force (NCIJTF) CyWatch 24/7 Command Center (contact: [cywatch@ic.fbi.gov](mailto:cywatch@ic.fbi.gov); 855-292-3937)

Dams Sector Resources

* Dams Sector Publications (<https://www.cisa.gov/dams-sector-publications>)
* HSIN-CI Dams Portal (<https://www.cisa.gov/resources-tools/resources/hsin-ci-dams-portal>)
* Dams Sector Tabletop Exercise Toolbox (<https://www.cisa.gov/resources-tools/resources/dams-sector-tabletop-exercise-toolbox>)

State Level Resources

* Multi-State Information Sharing and Analysis Center (MS-ISAC) (contact: [info@msisac.org](mailto:info@msisac.org); 518-266-3460)
* National Governors Association (NGA) (<https://www.nga.org/>)
* NGA Center for Best Practices (<https://www.nga.org/bestpractices/divisions/hsps/>)
* DHS Fusion Centers (<https://www.dhs.gov/state-and-major-urban-area-fusion-centers>)
* National Association of State Chief Information Officers (NASCIO) (<https://www.nascio.org/>)

Private Sector/Business Resources

* InfraGard (<https://www.infragard.org/Files/InfraGard_Redesign_2-24-2022.pdf>)
* Internet Security Alliance (<https://isalliance.org/>)
* Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs) (<https://www.isao.org/information-sharing-groups/>)
* Water ISAC (<https://www.waterisac.org/>)
* Electricity ISAC (<https://www.eisac.com>)
* International Association of Certified ISAOs ([http://www.certifiedisao.org](http://www.certifiedisao.org/); contact: [operations@certifiedisao.org](mailto:operations@certifiedisao.org))
* National Council of ISACs ([https://www.nationalisacs.org](https://www.nationalisacs.org/))

Preparedness Resources

* Cyber Security Evaluation Tool (CSET) (<https://www.cisa.gov/downloading-and-installing-cset>)
* CISA Cross-sector Cybersecurity Performance Goals (<https://www.cisa.gov/cross-sector-cybersecurity-performance-goals>)
* NIST Cybersecurity Framework Tools (<https://www.nist.gov/cyberframework>)

1. “Computer Security Resource Center Glossary: Cyber Resilience,” National Institute of Standards and Technology, accessed August 2, 2023, <https://csrc.nist.gov/glossary/term/cyber_resiliency>. [↑](#footnote-ref-2)
2. FEMA, “Homeland Security Exercise and Evaluation Program,” January 2020, <https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep>. [↑](#footnote-ref-3)
3. NIST Cybersecurity Framework, v2.0 (CSF 2.0) via NIST’s CPRT, “ID.RA-02: Cyber threat intelligence is received from information sharing forums and sources,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=ID.RA-02>. [↑](#footnote-ref-4)
4. NIST CSF 2.0 via CPRT, “ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=ID.RA-01>. [↑](#footnote-ref-5)
5. NIST CSF 2.0 via CPRT, “GV.OC-04: Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=GV.OC-04>. [↑](#footnote-ref-6)
6. NIST CSF 2.0 via CPRT, “PR.AT-01: Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.AT-01>. [↑](#footnote-ref-7)
7. NIST CSF 2.0 via CPRT, “PR.PS-01: Configuration management practices are established and applied,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.PS-01>. [↑](#footnote-ref-8)
8. NIST CSF 2.0 via CPRT, “ID.RA-07: Changes and exceptions are managed, assessed for risk impact, recorded, and tracked,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=ID.RA-07>. [↑](#footnote-ref-9)
9. CISA, “Cyber Resource Hub,” <https://www.cisa.gov/cyber-resource-hub>. [↑](#footnote-ref-10)
10. NIST CSF 2.0 via NIST’s CPRT, “ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=ID.IM-04>. [↑](#footnote-ref-11)
11. NIST CSF 2.0 via CPRT, “PR.DS-11: Backups of data are created, protected, maintained, and tested,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.DS-11>. [↑](#footnote-ref-12)
12. NIST CSF 2.0 via CPRT, “GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=GV.RR-02>. [↑](#footnote-ref-13)
13. NIST CSF 2.0 via CPRT, “ID.IM: Improvement – Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=ID.IM>. [↑](#footnote-ref-14)
14. Bill Briggs, “Hackers Hit Norsk Hydro with Ransomware,” Microsoft.com, December 16, 2019, <https://news.microsoft.com/source/features/digital-transformation/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/>. [↑](#footnote-ref-15)
15. Patrick Lucas Austin, “This Company Was Hit by a Devastating Ransomware Attack – But Instead of Giving In, It Rebuilt Everything,” *Time*, July 14, 2021, <https://time.com/6080293/norsk-hydro-ransomware-attack/>. [↑](#footnote-ref-16)
16. Briggs. [↑](#footnote-ref-17)
17. Austin. [↑](#footnote-ref-18)
18. Frederik Tomesco, “Pro-Russian Group Takes Responsibility for Cyberattack on Hydro-Quebec,” *Montreal Gazette,* April 13, 2023, <https://montrealgazette.com/news/local-news/hydro-quebec-website-and-app-blacked-out-in-cyberattack>. [↑](#footnote-ref-19)
19. Tom Hegel and Aleksandar Milenkoski, “NoName057(16) – The Pro-Russian Hacktivist Group Targeting NATO,” Sentinel Labs, <https://www.sentinelone.com/labs/noname05716-the-pro-russian-hacktivist-group-targeting-nato/>. [↑](#footnote-ref-20)
20. Tomesco. [↑](#footnote-ref-21)
21. Georgetown University Information Security Office, “Least Functionality Guidelines,” [https://security.georgetown.edu/config-mgt-policy/least-functionality-guidelines/#:~:text=The%20principle%20of%20least%20functionality%20provides%20that%20information,integral%20to%20the%20operation%20of%20that%20information%20system.st Functionality Guidelines | University Information Security Office | Georgetown University](https://security.georgetown.edu/config-mgt-policy/least-functionality-guidelines/#:~:text=The%20principle%20of%20least%20functionality%20provides%20that%20information,integral%20to%20the%20operation%20of%20that%20information%20system.)”. [↑](#footnote-ref-22)